Establishment of CERTs/CSIRTs to Promote Resilience and Stability in Cyberspace

Brazil-EU Cyber Consultations
Preventing Conflict in Cyberspace

Dr. Cristine Hoepers
General Manager, CERT.br/NIC.br
cristine@cert.br

cert.br nic.br cgi.br

CERTs effectiveness is based on cooperation – This cooperation is based on trust

For the past 10 years, all forums referred to the establishment of CERTs' as a low hanging fruit

- ITU, OAS, IGF that I participated personally

At IGF during the 2014 and 2015 work of the *Best Practice Forum on Establishing CERTs for Internet Security* the common agreement was:

- **CERTs' work is based on mutual trust**
- **This work is fluid and has a lot of informality**
- **Where a State decides to create its CERT can help or hinder trust and cooperation**

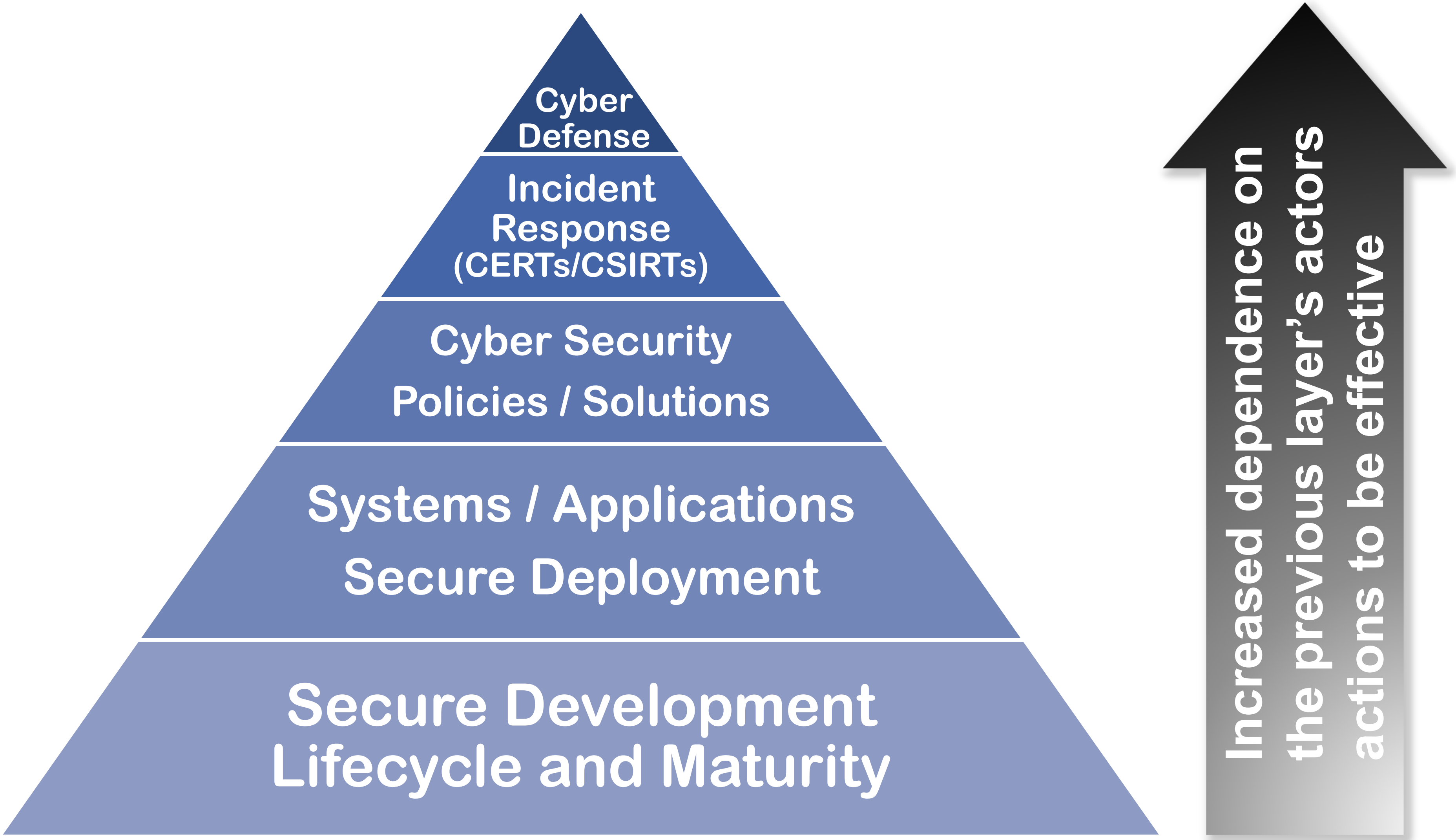
  https://www.intgovforum.org/multilingual/content/bpfs-archived-content

Main issues:

- **The existing strong cooperation is based on a delicate balance**
- **The CERT Community major preoccupation is that some political decisions can hinder and even stop the ability of teams to cooperate**

  Example: FIRST had to suspend 3 members due to US Sanctions

Poorly Designed and Developed Software: The Source of Most Evil



Cyber Defense

Incident Response (CERTs/CSIRTs)

Cyber Security Policies / Solutions

Systems / Applications Secure Deployment

Secure Development Lifecycle and Maturity

Increased dependence on the previous layer's actors actions to be effective

How to Improve: Short and Long Term Needs

Short term

- **Cyber Hygiene is key**
  - States should encourage technical best practices being drafted by working groups from FIRST, IETF, ISOC, IGF and RIRs
- **We need technical and effective CERTs**
  - FIRST is the Global Forum fostering cooperation worldwide

Long term

- **All industries need to commit to develop better products**
- **Regulators should**
  - forget certification of products
  - focus on minimum security requirements, including PSIRTs and prompt **security updates at scale**
  - examples to follow:

    https://www.m3aawg.org/CPESecurityBP

    https://www.internetsociety.org/wp-content/uploads/2019/11/IoT-Security-Platform-EN.pdf

Capacity Building: Short and Long Term Needs

Short term

- Transfer of knowledge among countries
- Learn with success cases
- Train current system and network operators on how to improve the security of their systems

Long term

- Change Universities Curriculum
  - Security by design and by default it is not part of the Engineering and Computer Science Courses
- We shouldn’t focus on Security degrees
- We need all areas and disciplines to include security in all phases of design and development

A Reflection on Real World Behavior:

Norms and Software [in]Security

cert.br nic.br cgi.br

UN GGE 2015 Report: **Responsible Vulnerability Disclosure**

13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following **recommendations for consideration by States** for voluntary, non-binding norms, **rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment**:

[...]

> (j) States **should encourage responsible reporting of ICT vulnerabilities** and **share associated information** on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

[...]

"*0-Days*" and Governments Stockpiling Vulnerabilities: **From *EternalBlue* to *WannaCry* – a self inflicted problem?**

2012 (before) – NSA discovers a Windows remote exploit, names it *EternalBlue* keeps it secret.

1st Semester/2016 – *The Shadow Brokers* have access to NSA data, including *EternalBlue*.

August 2016 – *The Shadow Brokers* starts publishing NSA tools on the Internet.

07 January 2017 – *The Shadow Brokers* starts selling NSA tools, including *EternalBlue*.

January/February 2017 – NSA contacts Microsoft with details of the vulnerability.

14 March 2017 – Microsoft releases MS17-010, fix for CVE-2017-0144 – the *EternalBlue*.

14 April 2017 – *The Shadow Brokers* releases 300MB of NSA material on Github, including *EternalBlue*.

12 May 2017 – *WannaCry* released, exploiting *EternalBlue*

https://boot13.com/windows/timeline-nsa-hacking-tool-to-wannacry/

https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Thank You

www.cert.br

@ cristine@cert.br

@certbr

November 21, 2019

nic.br cgi.br

www.nic.br | www.cgi.br